DREN

Service Agreement

1 May 2000

1 Purpose

This DREN Service Agreement (DSA) establishes the terms and agreements between the DREN Site Organization and the High Performance Computing Modernization Program (HPCMP) for use of the DREN. It documents the policies and procedures to be observed by the Site. The DSA constitutes the "contract" between the Site and the HPCMP. The DREN Site Organization and the DREN Site POC must concur with all terms of this DSA, as a prerequisite to receiving and retaining a DREN connection.

1.1 Concurrence – Concurrence is provided by submitting the signed Site Concurrence Letter attached at Attachment 1. It must be signed by the organizational authority responsible for the Site and by the DREN Site point of contact (POC). For contractor sites the DSA must additionally be signed by the sponsoring government organization which verifies that the contractor is required to meet the terms of this agreement and that such terms are within the scope of their contract.

2 Applicability

This Service Agreement applies to all Organizations receiving DREN services.

3 Definitions

3.1 DREN Site – The location (Post, Base, Station, contractor building, etc.) where DREN service is to be provided

3.2 DREN Site Organization – The organization responsible for the DREN service delivery point (SDP). The Site Organization must have authority to make the commitments that are required in this DSA.

3.3 DREN User Organization – The organization which has the requirement for DREN connectivity. In most cases this is the same as the Site Organization. However, at some sites, the Site Organization will be the organization that controls the local network infrastructure (for example, the Consolidated Network Communications Center (CNCC) for the Air Force or the Director of Information Management (DOIM) for the Army) which supports the User Organization.

3.4 Service Delivery Point (SDP) – The physical location where the DREN connects to the Site. Normally, an SDP will consist of one rack (or less) of Contractor-provided and installed equipment (ATM devices, routers, access termination equipment, security equipment, etc.) that provides the SDP interface.

3.5 DREN Site Point of Contact (POC) – The Site's representative who has the responsibility to ensure that the terms of this agreement are met and that the user organization's requirements, with respect to DREN connectivity, are met. Changes should be submitted to the DREN Program Office (See attachment 5).

3.6 DREN Project Manager (DREN PM) – The individual appointed by the Director, HPCMP, with overall responsibility for all aspects of the DREN.

3.7 DREN Intersite Services Contract (DISC) – The contract under which Network services are provided. AT&T is the contractor.

3.8 DISC Project Manager (DISC PM) – The Defense Information Services Agency (DISA) government individual responsible for the DISC. DISA manages the DISC for the HPCMP.

4 Documentation

This DSA contains the terms for using the DREN and delineates the POC responsibilities. Other relevant documentation include:

- The DREN Intersite Services Contract
- Specific Service Delivery Point (SDP) Plans
- The Site Survey Guide

5 DREN Operating Policies

5.1 Mission – The DREN's primary mission is to provide high speed connectivity for organizations with validated HPCMP projects. In addition the DREN supports 1) Department of Defense (DoD) science & technology (S&T) organizations, 2) DoD test and evaluation (T&E) organizations, 3) the Ballistic Missile Defense Organization and 4) DoD modeling and simulation (M&S) (non-S&T and non-T&E) organizations.

5.2 Acceptable Use – The Director of the High Performance Computing Modernization Program (HPCMP), acting on behalf of the Director, Defense Research and Engineering (DDR&E), is the governing authority in making determinations concerning acceptable use of the DREN. Acceptable use is governed by DoD regulations, including DoD Regulation 5500.7, particularly paragraph 2-301, which says (among other things), *"Federal Government communication systems and equipment (including ... electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only*." DREN services are intended to support efforts within the communities listed in the Mission (above) by providing appropriate access to scarce High Performance Computing resources. Additionally the DREN provides an infrastructure, which supports and fosters collaborative investigative efforts between DoD researchers, as well as between DoD researchers and related industrial and academic research institutions. Use of the DREN for other purposes is not acceptable.

5.2.1 Acceptable and encouraged uses of DREN resources include but are not limited to the following:

(1) Direct support of HPC mission research endeavors which require data transport as an enabling capability or infrastructure.
(2) Communication and exchange for professional development, to maintain currency, or to debate issues in a scientific field.
(3) Use for disciplinary-society, government-advisory, or standards activities related to the user's research activities.
(4) Any other administrative communications or activities in direct support of research or other acceptable mission areas.
(5) Communication with foreign researchers and educators in connection with research or instruction to the extent permitted by regulatory guidance.
(6) Announcements of new products or services for use in research or instruction, *but not advertising of any kind*.
(7) Communication incidental to otherwise acceptable use, except for illegal or specifically unacceptable use.

5.2.2 Unacceptable uses of DREN resources include but are not limited to the following:

(1) Use for for-profit activities, unless covered by a specifically acceptable use (for example, a for-profit contractor might be allowed to use the DREN in support of his government contract).
(2) Extensive use for private or personal business.
(3) Use for the conduct of or to aid in the conduct of illegal activities.
(4) Use which is intended to interfere with or disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of

computer worms or viruses, and using the network to attempt unauthorized entry to any other machine accessible via the network.

5.3 Management – Overall management and administration responsibility for the DREN lies with the DREN PM but requires a team effort. Close coordination between the HPCMO (primarily the DREN PM), the site DREN POCs, and DISC PM is a critical success factor. The DREN PM is the responsible for:

(1) Enacting policy issued by the HPCMO director.

(2) Overall coordination, planning and liaison activities between the DREN community, the DISC PM and the DISC contractor.

Individual site organizations are responsible for obtaining any required technical assistance not specifically provided for in this document.

5.4 DREN Connection Requirements – The Site Organization must complete all DREN Connection Requirements before a DREN connection will be provided.

5.5 Funding – Funding must be in place before any connection can be installed, either provided by the user organization or the HPCMP in the case of validated HPCMP users. The DREN PM will provide funding particulars once he and the Site Organization have come to an agreement that a DREN connection should be installed.

5.6 Appointment of DREN Site POC – The Site Organization will appoint a DREN Site POC and at least one alternate POC who are responsible for all issues involving the DREN. Roles and responsibilities are further defined in section 7. At Government Sites the POCs should be Government employees of the Site Organization. At all sites, government, contractor or other non-government, the POCs must be employees with the authority to discharge the roles and responsibilities of section 7 and ensure that all requirements of this DSA are met. POCs and alternates must be readily available, including via e-mail. The Site Organization must keep a current, accurate record of all DREN POCs which includes each persons name, address, telephone number, e-mail address, etc., and must inform the DREN PM, DISC PM, and AT&T Government Markets Customer Coordination Center (GMCCC) of all changes. This may be accomplished by letter or electronic mail to the addresses in Attachment 2.

5.7 Security

5.7.1 DISC Requirements – The digital data transfer services provided by the DISC are commercial services that are unclassified and unsecured. **All Site Organizations must acknowledge the unsecured nature of the DISC services and accept the attendant risks and implications for site and data security.** The Contract states:

(1) Protection of Data:

(a) The Contractor shall use best commercial practices to protect data from access by unauthorized persons while in transit between SDPs.

(b) As part of the information security management programs at two or more sites where active SDPs are installed, the Government may choose to encrypt data prior to delivery to an SDP, or may choose to employ security technologies (such as Kerberos, RFC 1510) or other security devices (such as FASTLANE).

(2) Network Integrity

(a) The Contractor shall employ accepted best commercial practices to protect data against sabotage or tampering by unauthorized persons while in transit between SDPs.

(b) The Contractor shall employ accepted best commercial practices to protect all Contractor-provided equipment, and information about the operation of such equipment, which are used to provide services under this Contract, from use, sabotage, intrusion, tampering, or denial of service attempts by unauthorized persons. In the event that the

Contractor detects that any such use, sabotage, intrusion, tampering, or denial of service attempt has occurred, the Contractor shall immediately notify the Government.

5.7.2 DREN Site Accreditation – DoD Directive 5200.28, Security Requirements for Automated Information Systems, 21 March 1988, establishes the authority for the DISA security accreditation process. DISA Instruction 630-230-19, Information Systems Security Program, July 1996, requires that all information systems regardless of classification or sensitivity will achieve compliance with the minimum-security requirements stated therein. **All DREN Sites must be accredited in accordance with this regulation.** Responsibility for the security accreditation resides with the DREN Site Designated Approving Authority (DAA).

5.7.2.1 Evidence of security certification is required as part of the accreditation process. Each site may use its own security certification team or request security certification service from the Defense Information Systems Agency (DISA). For some sites (for example HPCMP shared resource centers) the HPCMP will require a DISA certification before a final authority to connect is issued. The DREN PM will address this issue as part of the connection process.

5.7.2.2 If the security accreditation is not yet in place, the Site Organization DAA may issue an Interim Authority to Operate (IATO) for the site SDP. The IATO must be submitted to the DREN PM, along with a description of the tasks remaining in order to achieve full accreditation and a timeline for their implementation must be included as supporting documentation. The DREN PM will review the documentation and may at his/her discretion proceed with DREN connection process or withhold connection until the accreditation is complete.

5.7.2.3 All DREN sites must submit to Security Test and Evaluations (ST&E) and/or Site Assistance Visits (SAVs) if required by HPCMP. ST&Es and SAVs evaluate the security posture of the site. Currently only HPCMP shared resource centers have this requirement, but other sites may be inspected in the future.

5.7.2.4 The DREN PM will not authorize final connection to establish DREN connection until the HPCMO has received and approved security documentation as described in the DREN Connection Requirements.

5.7.2.5 If sensitive unclassified or classified information is to be transported using the DREN, the Site Organization must provide for protection of the information independent of the DISC. Site accreditation of the SDP must assert that measures are in place, which assure that the independent protection is adequately provided. For classified information, a MOA with any organization with whom data is exchanged must be provided. Responsibility for the security accreditation resides with the DREN Site Designated Approving Authority (DAA).

5.7.3 Monitoring – In accordance with the requirements of Chairman Joint Chief of Staff Instruction (CJCSI) 6510.01B, Defensive Information Operations Implementation, 22 August 1997, with change 1, 26 August 1998, and Defense Research and Engineering Network (DREN) connection requirements, the DREN is monitored for security purposes. All sites must sign Consent to Monitor Statement as part of the connection requirements. See Attachment 4.

5.7.4 DREN Security Requirements – All Sites are required to meet existing and future DREN security requirements. All DoD networks, including the DREN, are tightening and improving security in response to increased threats. DREN security requirements will generally be provided as "DREN Operating Procedures" but, for actions requiring prompt action, may also be communicated via e-mail or phone from the HPCMO. *Specifically the POC must ensure that the site is positioned to respond immediately to security requirements. These could include the requirement to limit service or disconnect from the DREN.*

5.7.4.1 Sites that host HPCMP shared resources are monitored by Network Intrusion Detection Systems (NIDSs). These sites must assist in management of the NIDs and respond to all incidents and events reported by the HPCMP Computer Emergency Response Team (CERT).

5.7.4.2 In the future, some or all *sites may be required to purchase, install, maintain and/or operate security equipment as directed by the DREN PM* (For example, intrusion detection systems, firewalls, security routers, encryption devices, etc.).

5.7.5 Service/Agency Security Requirements – DREN Sites must meet all security requirements imposed by their respective Service or Agency S/A. If the requirements of the mission for which the DREN connection is being obtained are incompatible with S/A requirements, an agreement with the S/A must be reached before a DREN connection will be approved.

6 DISC Services and Requirements

6.1 Types of Services/Connections – The DISC can provide connectivity to (nearly) any location within the 50 United States. Types of Service (e.g., IP or ATM, interface types, etc.) are listed in Attachment 4.

6.2 Management – DISC service management is performed by the Contractor (AT&T) and includes routine services including IP route management, ATM PVC setup and SVC signaling, service coordination (24 hours per day via the AT&T GMCCC), and certain automated monitoring. DISC services provided by AT&T include operation and maintenance of the SDP and DISC network infrastructure engineering.

6.3 Training – The DISC Contractor provides training when ordered as part of each SDP installation. Computer Based Training is available for site managers, site operators, and end-users (which includes the DREN POC) of the DISC services. Since all instruction is available as three site-licensed Computer Based Education modules, it is generally recommended that all three modules be ordered with every SDP ordered by the Subscriber Organization. All updates of these training modules (if required) are included in the initial order.

6.4 SDP Plans – Following receipt of an order for new or modified DISC service, the DISC Contractor will provide an SDP Plan as the first deliverable in accordance with the contract provisions. The Contracting Office and the DISC PM will coordinate the review and approval of the plan with the participation of the Site Organization and the HPCMO as applicable. The approved SDP Plan will provide the specific tasks and schedule to be executed by the Contractor in accomplishing the ordered installation or modification action.

6.5 SDP Equipment – According to the terms of the DISC, AT&T, or its designated sub-contractor, is required to provide all the equipment necessary to implement the service for the SDP, including the provision of all cable/fiber to the SDP and the equipment cabinet. There is no Government furnished equipment permitted under the DISC Contract.

6.5.1 The Site Organization must provide power, air conditioning, physical security and sufficient floor space available to accommodate the SDP cabinet. (Approximately 2 feet wide, 3 feet deep, 6 feet high.) Also see "Equipment Accountability", paragraph 7.5 below.

6.6 SDP Relocation – Periodically there is a requirement to relocate communications and automated data processing equipment to accommodate changes and expansions at the local level. Due to the nature of DISC services, it is imperative that the Site Organization follows these procedures for SDP relocation.

(1) If SDP relocation is required, contact the DREN PM who must approve and transfer the request to the DISC PM. Actual relocation, including all site survey work, site preparation, relocation, and service restoration, will be accomplished by the DISC Contractor. If the DREN

PM determines that the Site Organization is responsible for funding, those funds must be in place before the relocation will be authorized.

(2) *At no time is the site authorized to move DISC equipment without DISC PM approval.*

6.7 Logistics Support – In general, the Contractor is responsible for all logistics associated with services under the DISC. Spare equipment is generally kept and maintained by Contractor personnel.

(1) Technical assistance may be required at a DISC SDP. Such assistance will be provided by consultation with the AT&T GMCCC, see paragraph 7.4.

(2) There is no equipment acquired by the Government as a result of its using the DISC; however, the DREN POC may have custodial care responsibilities, see paragraph 7.5.

6.8 SDP Failure Reporting – In general, anyone who notices that the SDP is not operating properly may report the failure to the AT&T GMCCC. The person making the report must identify herself/himself, identify the organization and the geographical site, describe the perceived problem and stand ready to be contacted by the AT&T GMCCC for verification of the operational status of the SDP. The GMCCC is responsible for opening a trouble ticket upon notification, making a determination as to whether the SDP is out of service, and if so, make arrangements for its repair.

6.8.1 According to the Contract, the Contractor is required to make repairs within 2 hours (30 minutes during 0800-2000 hours EST). If the Contractor is not able to make repairs within this time period, the Government will receive service credits commensurate with a pre-established formula. It is incumbent upon the DREN POC to provide the Contractor timely access to the SDP so that service can be quickly restored. If the SDP is located in a facility that is not manned, the DREN POC must ensure that local, on-site assistance is provided upon receiving a request from the AT&T GMCCC. The DREN POC must notify the AT&T GMCCC whenever a site cannot be entered outside of normal duty hours.

6.9 SDP Routine Operational Services – The DREN POC and any identified alternate(s) are the only persons authorized to request Routine Operational Services (ROS) from the GMCCC for the local SDP. The DREN POC and alternate(s) must be registered with the AT&T GMCCC and the DISC PM, as described in paragraph 7.3, before any ROS requests can be accepted.

6.9.1 The person making an ROS request must be authenticated by the GMCCC using the following process:

(1) The requester calls the GMCCC, states the desired ROS, and hangs up.

(2) The GMCCC, using a pre-stored telephone number will call back the individual.

(3) The individual will provide a previously registered identifying code (four characters) which will be matched by the GMCCC with its database. If a match exists, the ROS will be accepted, if not, the ROS will be denied.

6.9.2 Examples of Routine Operational Services that may be requested include: adding or removing IP routes (when applicable), accessing SDP interface and routing data residing in the Contractor's equipment, and accessing MIB selections.

7 DREN POC Roles and Responsibilities

The DREN POC has overall responsibility for the actions and tasks listed below. Designated alternates may fill-in at the request or in the absence of the POC. However, the DREN POC retains overall responsibility to ensure task/action completion.

7.1 DREN Policy – The DREN POC has primary responsibility for enforcement of all DREN Policy (see section 5 above).

7.2 Problem Resolution – The DREN POC is the primary response agent for all failure and troubleshooting activities and is responsible for on-site coordination with the technical support staff

to assure problems with the local communications infrastructure have, to the extent possible, been eliminated prior to escalation.

7.2.1 The POC must coordinate with local installation infrastructure authorities as applicable to ensure that DREN-related matters are brought to the attention of the proper local officials when their participation is a procedural requirement for problem resolution.

7.3 Registration to Request SDP Routine Operational Services – The DREN POC and any identified alternate(s) are the only persons authorized to request Routine Operational Services (ROS) from the GMCCC for the local SDP. The DREN POC and alternate(s) must be registered with the AT&T GMCCC and the DISC PM before any ROS requests can be accepted. Registration is accomplished separately by each individual sending their name, organization, phone number and a four digit identifying code (e.g., last four numbers of the SSN) to the AT&T GMCCC and the DISC PM.

7.4 On-Site Technical Assistance Responsibilities – The DREN POC must provide or arrange for on-site technical assistance to the AT&T GMCCC in the following areas:

7.4.1 Coordinate, at the SDP site, the physical site preparation and the installation and activation of the SDP, and access circuit equipment. This coordination includes interactions with the DISC PM, the DISC Contractor (or subcontractors) local telephone personnel, and Service/Agency Operation and Maintenance (O&M) or Engineering and Installation (E&I) activities. (Contractor personnel will install and configure any DISC equipment used to deliver SDP services.)

7.4.2 Arrange for connectivity between the DISC SDP and the local user's equipment.

7.4.3 Provide or arrange for operational assistance under the telephonic instruction of the AT&T GMCCC.

7.4.4 Coordinate and monitor scheduled and unscheduled corrective maintenance, and allow for scheduled preventive maintenance as directed by the AT&T GMCCC. The DREN POC must also coordinate authorized outages with his/her respective users and the AT&T GMCCC.

7.5 Equipment Accountability – The DREN POC is responsible for care and safekeeping of all installed DISC SDP equipment and equipment shipped to the SDP site for future installation. The SDP site equipment remains DISC Contractor property although it may be entered in the site's property book/equipment records for custodial purposes depending on Site Organization policies.

7.5.1 The DREN POC may be requested to provide or arrange for temporary storage of some SDP parts, assemblies, and materials. These items are expected to be relatively small, e.g. cable assemblies, modems, etc. Typically, this material will need to be retained for only a few days.

7.6 Site Access Control and Security

7.6.1 The DREN POC regulates access to the SDP site. The DISC PM will provide the DREN POC an initial roster of Contractor personnel who are authorized access to SDP equipment. The DREN POC should add names to this roster, as required by the DISC PM, and maintain a copy of the current access roster to the site's SDP equipment.

7.6.2 The DREN POC must ensure that no DISC SDP equipment is moved, interfered with, or tamper with, and that no maintenance, other than external cleaning, is performed unless directed by the AT&T GMCCC.

7.6.3 The DREN POC shall implement site physical security procedures as specified in applicable DoD and Service directives. Each SDP Plan will reflect the specific security requirements for a given site.

7.7 General Administration and Coordination – The DREN POC must:

7.7.1 Maintain up-to-date documentation including that issued by DISC PM and the DISC Contractor. This documentation will include a copy of the current SDP Plan to be delivered to the DREN POC during SDP activation.

7.7.2 Notify the office of the DREN PM of any situation, or any configuration changes to site equipment, which may impact DREN operations, including planned or unplanned outages.

7.7.3 Serve as focal point for SDP operations. The DREN POC must maintain close contact with all points-of-contact (i.e., users, AT&T GMCCC, local phone service personnel, etc.).

7.7.4 Maintain a list of telephone numbers, to support both liaison and local site assistance functions. This will include as a minimum, the AT&T GMCCC, the point-of-contact for directly-connected equipment (routers, ATM switches, etc.) at that site, and other telephone numbers such as those of the servicing telephone company, the local technical control, the local communications Operations & Maintenance (O&M) unit representative, and contract personnel responsible for equipment maintenance.

7.8 SDP Site Survey Assistance – DISC SDP site surveys are conducted by the DISC Contractor. These surveys require some support on the part of the host location. This support may represent the first contact on the part of the DREN POC with the various parties involved with set-up, test, and operations of the DISC SDP. The DREN POC should coordinate local assistance, as required, to successfully complete the site survey.

7.8.1 Prior to the site survey, the DREN POC will arrange for conference room space to be used by the survey team. The DREN POC will also ensure that all local organizations affected by the installation and operation requirements for the DISC SDP site attend the meeting about the site survey. At a minimum, this includes the DISC SDP hosting organization and local telecommunications personnel.

7.9 Review of SDP Plans – The DREN POC will coordinate a site review of the Contractor-submitted SDP Plan to verify that local requirements, obtained during the Site Survey, are met when requested by the DISC PM. The results of this review must be communicated to the DISC PM in coordination with additional related SDP Plan reviews.

7.10 SDP Testing and Acceptance

7.10.1 The DREN POC must witness the SDP Acceptance Testing conducted by the Contractor. This testing will be conducted when the SDP is initially installed, after a modification to the SDP, and after the SDP has been restored to operational condition following a failure. The AT&T GMCCC will notify the DREN POC of the schedule for the test.

7.10.2 The DREN POC must become thoroughly familiar with the SDP operation and be able to exercise the Analysis and Testing capabilities built into the SDP. These capabilities will aid the DREN POC in problem and fault isolation and in performance measurement and validation.

7.10.3 The DREN POC should be able, after training or with assistance from the AT&T GMCCC, to recognize what is considered to be normal operating conditions for the DISC SDP equipment. The DREN POC should report any abnormal conditions to the AT&T GMCCC.

7.10.4 The DREN POC may be required to participate in a Collective SDP test, which is a test of the Contractor's supporting infrastructure, if the site SDP is part of a collective test set.

7.10.5 The results of all observed testing will be communicated to the DISC PM in coordination with additional related SDP testing observations.

7.11 SDP and Circuit Installation Assistance

7.11.1 The DREN POC monitors the work of Government personnel, O&M command, the DISC contractors, and other commercial vendors supporting the DISC SDP site. The DREN POC will notify the DISC PM via telephone or electronic mail whenever Government personnel or Contractor work performance problems are observed or when the DREN POC suggests improvements to the DISC SDP site. The following minimum tasks should be completed by DISC SDP installation contractors prior to acceptance of the completed work:

(1) SDP equipment and access circuit installed according to the DISC SDP Plan.

(2) SDP is operational as determined by testing with the AT&T GMCCC.

(3) All equipment (racks, drawers, patch panels, cables, modems, etc.) is properly labeled.
(4) All technical documentation is on hand, correct, and coordinated with the AT&T GMCCC.

7.11.2 The DREN POC, in conjunction with vendors and/or Government Engineering and Installation (E&I) teams, will assist with:
(1) Identification of space to house SDP equipment.
(2) Circuit installations between the commercial vendor to the SDP.
(3) Identification of appropriate cross-connect points, circuit-wiring pairs required to complete an access circuit order.
(4) Circuit implementation coordinators, Service or Agency E&I activities, and commercial telephone company installation or maintenance personnel by coordinating the assignment of cable pairs or channels on local carrier systems for tail circuits as requested.

7.11.3 When requested by the DREN PM, DISC PM, or supporting contractors, the DREN POC will provide site status on SDP installations in process.

8 Renewal of Service Agreement

This DSA must be renewed every three years, at a minimum. It must also be renewed 1) whenever the DREN POC appointment changes (to ensure his/her acceptance of the responsibilities herein) or 2) upon request of the DREN PM (in the case of major changes in DREN policy or contractual requirements). Renewal is accomplished by a resubmitting the DREN Site Concurrence Letter as described in paragraph 1.1.

Attachment 1 to DREN Service Agreement

DREN SITE CONCURRENCE LETTER

STATEMENT OF AGREEMENT

1. Acknowledgment of Terms and Conditions

We acknowledge and understand the contents of the DISC Service Agreement and agree to comply with the DISC Operating Policies and to the roles and responsibilities contained therein for the DISC Site POC.

2. Acknowledgment of unclassified and non-secure service

We acknowledge and understand that the DISC services are unclassified and non-secure with attendant risks. We acknowledge that data protection is provided by best commercial practices against unauthorized access and sabotage, etc. while transiting the Contractor's infrastructure.

3. Acknowledgment of explicit security policy

We acknowledge and understand that we are responsible for compliance with DoD 5200.28 or DoD 5220.22-M (contractor sites). Specifically we have developed and implemented a written Security Plan/Policy which governs users and systems connected to the DREN.

DREN POC:

Signature _____ *Date* _____

Name _____ *Ident. Code* _____

Organization _____

Site Organization Commander/Director:

Signature _____ *Date* _____

Name _____

Organization _____

Title _____

Government Sponsor (for Contractor sites only) verifies that the contractor is required to meet the terms of this agreement and that such terms are within the scope of their contract.

Attachment 2 to DREN Service Agreement

Point of Contact Information

DREN Program Manager

DREN Program Manager / Rodger Johnson
1010 North Glebe Rd, Suite 510
Arlington, VA 22201-4795
Coml.: 703-812-8205, Fax: 703-812-9701
E-mail: rjohnson@hpcmo.hpc.mil

DISC Project Manager

DISC Project Manager / Ralph Dwyer
DISA/Code D311/DISC PMO
10701 Parkridge Blvd
Reston, VA 20191-4357
DSN: 653-3241, Coml.: 703-703-735-3241, Fax: 703-735- 3207
E-mail: dwyerr@ncr.disa.mil

AT&T GMCCC

DISC Government Markets Customer Coordination Center (GMCCC)
Attn: Mr. Jim Baird
3033 Chain Bridge Rd
Oakton, VA. 22185
E-mail: jellybean@ems.att.com

E-mail: noc@att-disc.net
Telephone: 1-888-DISC-USA (347-2872)
FAX: 703-691-6362

DREN Security Action Officer

DREN Security Action Officer / Joseph Molnar
High Performance Computing Modernization Office
1010 Glebe Road, Suite 510
Arlington, VA 22201-4795
Coml.: 703-812-8205, Fax: 703-812-9701
E-mail: molnar@hpcmo.hpc.mil

Attachment 3 to DREN Service Agreement

Consent to Monitor Statement
[This statement may be placed on organizational letterhead and formatted in accordance with organizational requirements. However, the content must not be changed]

MEMORANDUM FOR HIGH PERFORMANCE COMPUTING MODERNIZATION OFFICE

SUBJECT: CONSENT TO MONITOR FOR DREN

In accordance with the requirements of Chairman Joint Chief of Staff Instruction (CJCSI) 6510.01B, Defensive Information Operations Implementation, 22 August 1997, with change 1, 26 August 1998, and Defense Research and Engineering Network (DREN) connection requirements, we acknowledge that the DREN program office, or its designated representative, will conduct periodic monitoring of the DREN. We acknowledge and consent to initial and periodic assessments of all connected systems and networks to determine the security features in place to protect against unauthorized access or attack. We accept the responsibility to notify all users, who access the DREN through our connection to the DREN, of these monitoring and assessment requirements.

<DAA or Commander Signature>

<DAA or Commander Signature Block>

Attachment 4 to DREN Service Agreement

Types of Service Available on the DISC

Table 1. SDP CONFIGURATION & ORDERING OPTIONS FOR EACH SDP TYPE

The following sub-tables display all possible SDP ordering selections and corresponding CLINs that must be used.

Table 1-1a. List of Possible Ordering Selections for Type-1 IP SDPs

IP Ordering Selection ID	IP SDP Type	SUBSCRIPTION				ACCESS
		Protocol	Physical Interface		Bandwidth (Mbps)	
01 §	E.1	Ethernet	AUI		BW=3/8	2xDS-1
02	E.1	Ethernet	AUI		BW=3/8	DS-3
03 §	E.1	Ethernet	10Base-T		BW=3/8	2xDS-1
04	E.1	Ethernet	10Base-T		BW=3/8	DS-3
05 §	E.1	Ethernet	10Base-2		BW=3/8	2xDS-1
06	E.1	Ethernet	10Base-2		BW=3/8	DS-3
07 §	E.1	Ethernet	10Base-F		BW=3/8	2xDS-1
08	E.1	Ethernet	10Base-F		BW=3/8	DS-3
09	E.2	Ethernet	100Base-T		BW=10.2/25.4 (Heartbeat for #11)	DS-3
10	E.2	Ethernet	100Base-T		BW=10.2/25.4 (Heartbeat for #12)	OC-3
11 §	E.3	Ethernet	100Base-T		BW=30/80	DS-3
12	E.3	Ethernet	100Base-T		BW=30/80	OC-3
13	F.1	Fiber DDI	Single Attchd Sta	Single-mode fiber	BW=10.2/25.4 (Heartbeat for #25)	DS-3
14	F.1	Fiber DDI	Single Attchd Sta	Single-mode fiber	BW=10.2/25.4 (Heartbeat for #26)	OC-3
15	F.1	Fiber DDI	Single Attchd Sta	Multi-mode fiber	BW=10.2/25.4 (Heartbeat for #27)	DS-3
16	F.1	Fiber DDI	Single Attchd Sta	Multi-mode fiber	BW=10.2/25.4 (Heartbeat for #28)	OC-3
17	F.1	Fiber DDI	Dual Attchd Sta	Single-mode fiber	BW=10.2/25.4 (Heartbeat for #29)	DS-3
18	F.1	Fiber DDI	Dual Attchd Sta	Single-mode fiber	BW=10.2/25.4 (Heartbeat for #30)	OC-3
19	F.1	Fiber DDI	Dual Attchd Sta	Multi-mode fiber	BW=10.2/25.4 (Heartbeat for #31)	DS-3
20	F.1	Fiber DDI	Dual Attchd Sta	Multi-mode fiber	BW=10.2/25.4 (Heartbeat for #32)	OC-3
21	F.1	Copper DDI	Single Attchd Sta	High-Perf Twisted Pr	BW=10.2/25.4 (Heartbeat for #33)	DS-3
22	F.1	Copper DDI	Single Attchd Sta	High-Perf Twisted Pr	BW=10.2/25.4 (Heartbeat for #34)	OC-3
23	F.1	Copper DDI	Dual Attchd Sta	High-Perf Twisted Pr	BW=10.2/25.4 (Heartbeat for #35)	DS-3
24	F.1	Copper DDI	Dual Attchd Sta	High-Perf Twisted Pr	BW=10.2/25.4 (Heartbeat for #36)	OC-3
25 §	F.2	Fiber DDI	Single Attchd Sta	Single-mode fiber	BW=30/80	DS-3
26	F.2	Fiber DDI	Single Attchd Sta	Single-mode fiber	BW=30/80	OC-3
27 §	F.2	Fiber DDI	Single Attchd Sta	Multi-mode fiber	BW=30/80	DS-3
28	F.2	Fiber DDI	Single Attchd Sta	Multi-mode fiber	BW=30/80	OC-3
29 §	F.2	Fiber DDI	Dual Attchd Sta	Single-mode fiber	BW=30/80	DS-3
30	F.2	Fiber DDI	Dual Attchd Sta	Single-mode fiber	BW=30/80	OC-3
31 §	F.2	Fiber DDI	Dual Attchd Sta	Multi-mode fiber	BW=30/80	DS-3
32	F.2	Fiber DDI	Dual Attchd Sta	Multi-mode fiber	BW=30/80	OC-3
33 §	F.2	Copper DDI	Single Attchd Sta	High-Perf Twisted Pr	BW=30/80	DS-3
34	F.2	Copper DDI	Single Attchd Sta	High-Perf Twisted Pr	BW=30/80	OC-3

IP Ordering Selection ID	IP SDP Type	SUBSCRIPTION				ACCESS
		Protocol	Physical Interface		Bandwidth (Mbps)	
35 §	F.2	Copper DDI	Dual Attchd Sta	High-Perf Twisted Pr	BW=30/80	DS-3
36	F.2	Copper DDI	Dual Attchd Sta	High-Perf Twisted Pr	BW=30/80	OC-3

§ Symbol indicates this Ordering Selection does not meet the "tens of minutes" requirement for maximum rate transfers (see SOW paragraph 3.1.2.b). For those customers who do not need bursting capabilities for long durations (i.e., bursting for milliseconds as opposed to "tens of minutes"), AT&T offers alternative access selections for E.1, E.2, E.3, F.1 and F.2 SDP types which may be more cost effective; for instance, the customer may elect to use the 2xDS-1 based access arrangement to support an E.1 SDP rather than a DS-3; likewise the customer may elect to use DS-3 access for the E.3 and F.2 SDPs rather than OC-3. It should be noted, however, that to meet the bursting requirement for "tens of minutes", the higher access rate alternative should be selected for an SDP type. Thus, if the customer wants an E.1 SDP and anticipates bursting for "tens of minutes", the customer should order the DS-3 access alternative. Also, if the customer will want to convert from a "Heartbeat" service to a "Highest Capability" service such as from F.1 to F.2 (or from E.2 to E.3) and there is a bursting requirement for "tens of minutes" then the OC-3 access arrangement should be ordered with the F.1 (or E.2) SDP.

Table 1-2a. List of Possible Ordering Selections for Type-2 ATM SDPs

ATM Ordering Selection ID	ATM SDP Type	SUBSCRIPTION		ACCESS
		Physical Interface	Aggregate Cell-Rate	
01	DS3.0	DSX-3	4 kc/s HB (Heartbeat for #02, 03, 04, 05)	DS-3
02	DS3.1	DSX-3	16 kc/s	DS-3
03	DS3.2	DSX-3	32 kc/s	DS-3
04	DS3.3	DSX-3	64 kc/s	DS-3
05	DS3.4	DSX-3	96 kc/s	DS-3
06	DS3.5	OC-3c	96 kc/s	DS-3
07	OC3.0	OC-3c	16 kc/s HB (Heartbeat for #07, 08, 09,10)	OC-3
08	OC3.1	OC-3c	64 kc/s	OC-3
09	OC3.2	OC-3c	96 kc/s	OC-3
10	OC3.3	OC-3c	128 kc/s	OC-3
11	OC3.4	OC-3c	256 kc/s	OC-3
12	OC12.0	OC-12c	64 kc/s HB (Heartbeat for #12, 13, 14)	OC-12
13	OC12.1	OC-12c	256 kc/s	OC-12
14	OC12.2	OC-12c	500 kc/s	OC-12
15	OC12.3	OC-12c	1000 kc/s	OC-12
16	OC48.0	OC-48c [WCA]	256 kc/s HB (Heartbeat for #16, 17, 18)	OC-48
17	OC48.1	OC-48c [WCA]	1000 kc/s	OC-48
18	OC48.2	OC-48c [WCA]	2000 kc/s	OC-48
19	OC48.3	OC-48c [WCA]	4000 kc/s	OC-48

Note: [WCA] means When Commercially Available

Attachment 5 to DREN Service Agreement

DREN PRIMARY POC:

NAME	
ADDRESS	
PHONE	
FAX	
DSN	
E-MAIL	

DREN SECONDARY POC:

NAME	
ADDRESS	
PHONE	
FAX	
DSN	
E-MAIL	

DESIGNATED APPROVAL AUTHORITY:

NAME	
ADDRESS	
PHONE	
FAX	
DSN	
E-MAIL	

SITE SECURITY MANAGER:

NAME	
ADDRESS	
PHONE	
FAX	
DSN	
E-MAIL	